INFORMATION SECURITY GUIDE FOR STUDENTS

August 2009

CONTENTS

The purpose of information security and data protection.....1
Access rights and passwords 2
Internet and e-mail 3
Privacy protection 5
University's computers and IT security.....6
Personal computers and IT security 8
Public computers and wireless networks 9
Portable memory devices and backup copies 10
Copyrights and software licenses 11
When your right to study expires 12
Malware infections and information security breaches 13
Further information and useful links ..... back cover

This Information Security Guide is primarily written for university students. The authors wish to thank the Government Information Security Management Board (VAHTI), whose Information Security Instructions for Personnel (VAHTI 10/2006) set an example for and inspired the writing of this guide. We also wish to thank SEC, the information security team of Finnish universities, for commenting on the guide.

Authors: Kenneth Kahri (Univ. of Helsinki), Olavi Manninen (Univ. of Kuopio), Kaisu Rahko (Univ. of Oulu).
Layout and photos: Katja Koppinen and Raija Törrönen (Univ. of Kuopio).
English translation: Anna Naukkarinen (Tampere Univ. of Technology).

This guide has been written as part of official duties of employment at the universities of Helsinki, Kuopio and Oulu and is licensed under a Creative Commons Attribution-Noncommercial-Share Alike License:
http://creativecommons.org/licenses/by-nc-sa/1.0/fi/.

THE PURPOSE OF INFORMATION SECURITY AND DATA PROTECTION

- Computers and the Internet are important tools for students. However, there are certain risks involved in using the Internet, so you should be aware of the basic principles of information security and data protection.

- **Information security** means protecting information and information systems from unauthorized access and ensuring that they are reliable and safe to use.

- **Data protection** means protecting your information from unauthorized disclosure and preventing misuse of personal information.

- To protect your privacy, it is vital you take the principles of data protection into account when using a computer. Remember to protect both your own data and that of others. Information that needs to be protected from outsiders includes, for example, personal, contact, health and bank account information, e-mails and photographs.

- Information security is often considered difficult, but with common sense and by following instructions you can easily avoid most of the pitfalls.

- Everyone is responsible for maintaining information security at the university. The information security policies in force at Finnish universities stipulate that students are, for example, responsible for following given instructions to protect their own information and that of others. Information security breaches may have legal consequences.

- If you hold a position of trust alongside your studies, your responsibilities go beyond those of an ordinary student. Please familiarize yourself with these responsibilities.

ACCESS RIGHTS AND PASSWORDS

- Your access rights to the university's information systems are granted for your personal use only.

- Students usually log in to the university's computers and information systems with a username and password. Handle your username and password with as much care as your bank card.

- Some Finnish universities employ a smart card (student card Lyyra) for identification purposes and access control. Students must handle the smart card with care. As the owner of the card, you are responsible for the use of your smart card, so do not lend it to others.

- You are responsible for all the activities occurring under your user account. Do not tell your username or password to others. Even the system administrators do not need to know your password. Never provide your username and password in response to an unsolicited request.

- The university offers you e-mail and other services that are primarily meant to be used for study-related purposes. Reasonable use of the services for private purposes is allowed, provided that it does not hinder the primary purpose of the services.

- Using the university's information systems for commercial purposes is generally prohibited. Using the systems for political purposes, such as electoral campaigning, is similarly prohibited.

- A good password is easy to remember and hard to guess. Learn your password by heart and avoid writing it down.

- Do not use ordinary words or words that are, for example, derived from your name as your password. Select a password that includes lower case and upper case letters, numbers and special characters. Please note, however, that not all systems accept special characters as part of a password. For more information, please see the university's rules and regulations.

- After the university's IT Helpdesk sends you a new password, change it immediately into a password that only you know.

- Change your passwords regularly and follow the recommendations issued by the university. Change your password without delay, if you suspect it has been exposed. Do not use the same password in the university's information systems and external systems.

INTERNET AND E-MAIL

- Data is often transmitted through an insecure connection on the Internet. In such case, your data is not protected in any way, so be careful when using e-mails and the Web.

- Each student receives a user account and e-mail address from the university. The address provided by the university must be used as the primary e-mail address in all the university's services and information systems, including the Student Register and virtual learning environments (Oodi, Optima, Moodle, Blackboard, etc.).

- When you are writing e-mails and interacting with others through the Internet, remember to follow the principles of Netiquette. Posting insulting messages on an Internet forum is impolite. In some cases it may even result in a court sentence.

- E-mail attachments may be infected with malware. Beware of all unusual e-mails and especially e-mail attachments. Do not open suspicious e-mails. For more information, please contact the university's IT Helpdesk.

- Unsolicited advertisements and chain letters are spam. Do not answer to such e-mails or forward them. Instead, delete them immediately. Spam e-mails may contain malware or direct the user to a malicious website.

- Universities use different methods to filter spam. In some systems spam filtering is automatically enabled, and in others the user may have to enable filtering. For more information, please see the university's rules and regulations.

- Use caution with e-mails. The sender of the e-mail may be someone else than the person whose name shows up in your inbox. Viruses may also send e-mail without any user action.

- Be especially careful with so-called phishing e-mails. These fraudulent messages may ask for your username and password or online bank account information by giving some excuse that sounds reasonable or masquerading as a trustworthy entity.

- If you receive an e-mail that is not meant for you, please notify the sender that s/he has the wrong e-mail address. Remember that you are bound by confidentiality with regard to the content of the message.

- When you send e-mails, make sure you know the recipient's correct e-mail address. Check the address for typos before sending the message.

- Use caution when sharing your e-mail address or posting it on the Internet. Get yourself a free e-mail address, such

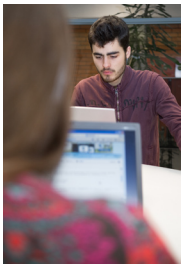
as a Hotmail or Gmail address. Avoid using your university e-mail address on Internet forums and services such as Facebook, MySpace, etc.

- Use only network services that are well-known and reliable.

- If you use an e-mail service provided by and external service provider, select a service that encrypts data transmission (letters https:// appear in the address bar and there is a lock icon on the bottom of the screen).

- Never use network services under a user account that has administrator privileges (Administrator, root).

PRIVACY PROTECTION



- Use caution when managing personal information. Think first what kind of personal information you can share with others and who is the recipient.

- You have the right to share your own personal information with others, but you need permission or other authorization to share anyone else's personal information.

- Be careful when posting personal information on yourself or others on Internet forums (e.g. Facebook, MySpace) or other network services. Once you post personal information, such as a photograph or home address, on the Internet it may be difficult or impossible to remove it completely afterwards.

- It is easy to impersonate someone else when using an Internet service, so do not believe everything you read.

- If you use your mobile phone in a public space, someone may hear and recognize you. Keep your voice down when speaking on the phone in public.

UNIVERSITY'S COMPUTERS AND IT SECURITY

- Do not let others see your computer keyboard or screen when you are typing your username and password or when you are processing sensitive data.
- Always log in to the university's computers with your own username and password. Log off after using a computer and make sure of the following:
- Delete all temporary files and other data saved by the browser.
- Delete other temporary files you have saved on the computer.
- Remember to take your memory stick and papers with you as you leave.
- If you need to leave the computer temporarily, take your memory stick and other materials with you and lock the computer, so no one will be able to see your username and password or read your files. Please note that locking the computer for a longer period of time may be prohibited at your university, because it reserves the computer and others cannot use it in your absence.

Locking your Windows computer (Win + L).

- Save all important data to your network drive or home directory when using a computer connected to the university's network. The university will then take care of saving a backup copy of your work.

- Save changes on a regular basis (in many Windows programmes with the key combination Ctrl + S), when you are modifying text or other material for a longer period of time. This way, you will not lose all your work in case of a technical failure.

- Before you print materials out of a shared printer, make sure you know where the printer is located. Collect your printouts as soon as possible. Lock the computer before collecting your printouts.

- The university's computers are meant to be used primarily for study-related purposes. If others are waiting for their turn, do not use a computer for personal purposes.

- Installing software on the university's computers is generally prohibited and often technically prevented, too. If you need certain software, please contact the IT Helpdesk. It is possible that the software has already been installed on computers in another classroom, or the university may in some cases agree to obtain a license for the software.

- If you have access rights to locked computer classrooms at the university, remember to close the door after entering and leaving the classroom. Do not let others into the classroom, if you are not sure they have the right to use the university's computers.

PERSONAL COMPUTERS AND IT SECURITY

- The university is responsible for the information security of its own computers. You are responsible for the information security of your own computer. Try to follow good administration practices.

- Good information security practices require that up-to-date firewall and antivirus software are installed on your computer, automatic update of the operating system (e.g. with the Windows update functionality) is enabled and security updates are carried out.

- Use a user account that has administrator privileges (e.g. Administrator, root) only to install software and manage user accounts.

- For normal use, create yourself a user account without administrator privileges. This improves privacy protection and decreases the risk of malware infection.

- Install new software on your computer only if it is absolutely necessary. Each unnecessary installation increases the risk of malware infection. Install software only from known software resources.

- Remember to make regular backup copies of your files. Think about what kind of data you could lose, if your hard disk is damaged or files are destroyed due to malware.

- Be careful when transporting and storing a laptop. The laptop needs to be protected from shock damage, dust and moisture. Never leave your laptop visible in a car.

- If you have your own wireless network connection, enable the security settings so others cannot use your connection or follow what you are doing on the Internet. For instructions, please see the user manual of your wireless device.

- If you have your own broadband connection, check the user manual to see if it includes a firewall and enable it.

- Keep track of warnings (issued, for example, by service providers) concerning information security threats (e.g. www.cert.fi/en/).

PUBLIC COMPUTERS AND WIRELESS NETWORKS

- Computers in Internet cafes, libraries and other public spaces are handy when you are on the go and need to use a computer. However, be sceptical of information security and data protection when using such computers. The computer may be infected with malware as a result of the activities of the previous user.

- Think first if it is necessary to log in to network services with your own username and password, and consider what kind of data to process with a publicly-accessible computer.

- Using a computer always leaves tracks behind: temporary files, cookies, browser sessions, etc. Learn how to clear the cache memory of a browser and other typical tracks that using a computer leaves.

- When you are using wireless networks, find out if the connection is secure or not. Networks in shared use, such as computers in cafes and airports, usually have an unprotected connection and others can easily monitor what you are doing online. When you are using these kinds of networks, use only e-mail and network services that encrypt transmission (letters https:// appear in the address bar and there is a lock icon on the bottom of the screen.

PORTABLE MEMORY DEVICES AND BACKUP COPIES

- The university will take care of saving backup copies of your files, if you save the data to your network drive or your home directory on the university's server.

- USB memory sticks are convenient, but do not use them as the primary or only medium to save your data. A memory stick is easily lost – do not save sensitive data on a memory stick.

- Be careful with using other people's USB memory sticks. The memory stick may be infected with malware. When you insert the memory stick into your computer, the malware may be automatically run and your computer will also get infected.

- If you find someone else's memory stick on campus, please deliver it to the IT Helpdesk without inspecting the contents.

- If you have a computer of your own, remember to make backup copies on a regular basis. Suitable backup media are, for example, USB hard disks, memory sticks and writable DVD or CD disks. Write down what information the backup copy contains and when the data was saved. Check regularly that your backup copies are still readable.

- Store backup copies in a separate place away from your computer, preferable under lock and key.

- Learn to keep your materials organised on the computer, memory devices and in paper form, so that it is easier to ensure they are protected.

- Old hard disks, memory sticks and other memory devices, and papers containing sensitive data should not be thrown in the bin. Destroy the materials appropriately: data saved

on a memory stick, hard disk or other electronic media is destroyed by overwriting or crushing the object, and paper documents are shredded.

COPYRIGHTS AND SOFTWARE LICENSES

- Only install licensed software, or freely available software, on your computer. Do not install illegal copies or any other software, if you are not sure you have the right to use it.

- The right to study at a university entitles students to use certain software. For further information, please see the university's rules and regulations.

- Remember that using software, to which you have access because of your student status, is often limited to study-related purposes. Your right to use the software will terminate when your right to study at the university expires. After this, it is your responsibility to uninstall the software from all the computers on which you have installed it.

- The terms of use concerning electronic resources available at the university's library restrict who has the right to use the resources and to what purpose. For further information, please see the instructions of the university's library.

- Films and music are protected by copyright. Do not download them from the Internet or share them through the Internet without the express consent of the person who owns the copyright. Current copyright legislation prohibits copying computer software for personal use. Unauthorized distribution of software protected by copyright is also punishable by law.

- When you are quoting someone else's material in your own written works or theses, you must follow the rules of citation. Always add a citation when you are quoting someone else's work. Always ensure you have the right to do so before quoting or inserting links to someone else's material into your own work.

WHEN YOUR RIGHT TO STUDY EXPIRES

- Your right to use the IT services available at the university will terminate when your right to study expires.

- After you graduate or your right to study expires, your right to use the university's IT services will be terminated. Your user account is usually disabled automatically. After your right to study expires, the university will permanently delete your user account, e-mails and files saved to your home directory after a certain period of time. Before your user account is disabled, please note the following:

  - Notify your friends that your e-mail address has changed.

  - Copy the files that you want to keep from the university's servers and delete the remaining files.

  - Copy the e-mail messages you want to keep or forward them to another e-mail address.

  - Uninstall any software, to which you had usage rights due to your student status and are no longer entitled to use, from your computer.

MALWARE INFECTIONS AND INFORMATION SECURITY BREACHES

- If you suspect that a computer is or has been infected with malware:

  1. Use another computer to change all the passwords you have used on the infected computer. If you have used online banking services through the infected computer, notify your bank immediately that your online bank account information may have been exposed.

  2. If the infected computer is your own, stop using it immediately and find out how to remove malware. If someone else owns the computer, contact the owner without delay.

- The university's IT Helpdesk may offer some limited assistance with restoring your computer after a malware infection. You can start by viewing instructions issued by the IT Helpdesk on handling computer viruses. In addition, visit the website of the company that developed your antivirus software for instructions on removing malware.

- If you have reason to suspect an information security breach or misuse of an information system, contact the person in charge of the service or IT system. If the case concerns your university, contact the IT Helpdesk. If the case concerns another organisation, contact the organisation's switchboard. Remember to leave your contact information, so you can be reached if additional information is needed.

FURTHER INFORMATION AND USEFUL LINKS

- Rules, regulations and information security policy of your university
- Instructions on using the Internet safely
  - » www.tietoturvaopas.fi/en/
  - » www.tietoturvakoulu.fi/en/
- Instructions on protecting your privacy and disclosing personal information
  - » www.tietosuoja.fi > in English
- Netiquette: good manners on the Internet
  - » www.en.wikipedia.org/wiki/Netiquette
- Instructions on secure data transmission, notifications of information security threats
  - » www.cert.fi/en/
- Information security guidelines for mobile phone users
  - » www.ficora.fi/mobiiliturva/english/
- The government's legislative data bank FINLEX
  - » www.finlex.fi/en/
- ICT Driving License Course Material (Univ. of Helsinki)
  - » www.helsinki.fi/tvt-ajokortti/english/